CLAIMS

1. A device authentication system comprising a terminal device including confidential information for device authentication and an authentication server for granting device authentication to the terminal device using the confidential information, wherein

the terminal device acquires a random number and generates a conversion value by converting a set of the acquired random number and the confidential information using a one-way function;

the authentication server acquires the random number acquired by the terminal device, the confidential information of the terminal device, and the conversion value generated by the terminal device;

a conversion value is generated by converting the set of the acquired random number and the confidential information using the same one-way function as that used by the terminal device; and

the conversion value generated by the terminal device is compared with the conversion value generated by the authentication server.

2. The terminal device that is granted device authentication in the device authentication system according to claim 1, comprising:

reception means for receiving from the authentication server a random number and random-number identification information for identifying the random number;

conversion means for generating a conversion value by converting a set of the received random number and the confidential information using a one-way function; and

transmission means for transmitting the generated conversion value, the received random-number identification information, and confidential-information identification information for identifying the confidential information in the authentication server.

3. The authentication server for granting device authentication to the terminal device according to claim 2, comprising:

random-number acquisition means for acquiring a random number;

transmission means for transmitting to the terminal device the acquired random number and random-number identification information for identifying the random number;

reception means for receiving from the terminal device a conversion value, the random-number identification information, and confidential-information identification information;

random-number identification means for identifying the random number transmitted to the terminal device using the received random-number identification information;

confidential-information identification means for identifying the confidential information of the device terminal using the received confidential-information identification information;

conversion means for generating a conversion value by converting a set of the identified confidential information and the random number using the same one-way function as that used by the terminal device; and

device authentication means for granting device authentication to the terminal device using the received conversion value and the generated conversion value.

4. A service server included in the device authentication system according to claim 1, the service server providing a service to the terminal device via device authentication by the authentication server, the service server comprising:

random-number acquisition means for acquiring a random number;

random-number transmission means for transmitting the acquired random number to the terminal device;

reception means for receiving from the terminal device a conversion value generated using the confidential information and confidential-information identification information;

random-number identification means for identifying the random number transmitted to the terminal device;

authentication-information transmission means for transmitting, to the authentication server, authentication information including the received conversion value, the confidential-information identification information, and the identified random number; and

authentication-result reception means for receiving from the authentication server a result of authentication based on the transmitted authentication information.

5. The terminal device receiving a service from the service server according to claim 4, comprising:

random-number reception means for receiving a random number from the service server;

conversion means for generating a conversion value by converting a set of the received random number and the confidential information by the use of a one-way function; and

transmission means for transmitting the generated conversion value and confidential-information identification information for identifying the confidential information in the authentication server.

6. The authentication server for granting device authentication to the device terminal when the service server according to claim 4 provides a service, the authentication server comprising:

reception means for receiving, from the service server, authentication information including a conversion value, confidential-information identification information, and a random number;

confidential-information identification means for identifying the confidential information of the terminal device by the use of the received confidential-information identification information;

conversion means for generating a conversion value by converting a set of the received random number and the identified confidential information by the use of the same one-way function as that used by the terminal device; and

device authentication means for granting device authenticating to the terminal device by the use of the received conversion value and the generated conversion value.

7. A terminal device method used by the terminal device that is granted device authentication in the device authentication system according to claim 1, the terminal device including a computer having reception means, conversion means, and transmission means, the terminal device method comprising:

a reception step of receiving from the authentication server a random number and random-number identification information for identifying the random number by the reception means;

a conversion step of generating a conversion value by converting a set of the received random number and the confidential information using a one-way function by the conversion means; and

a transmission step of transmitting the generated conversion value, the received random-number identification information, and confidential-information identification information for identifying the confidential information in the authentication server by the transmission means.

8. An authentication method used by the authentication server for granting device authentication to the terminal device according to claim 2, the authentication server including a computer having random-number acquisition means, transmission means, reception means, random-number identification means, confidential-information identification means, conversion means, and device authentication means, the authentication method comprising:

a random-number acquisition step of acquiring a random number by the random-number acquisition means;

a transmission step of transmitting to the terminal device the acquired random number and random-number identification information for identifying the random number by the transmission means;

a reception step of receiving from the terminal device a conversion value, the random-number identification information, and confidential-information identification information by the reception means;

a random-number identification step of identifying the random number transmitted to the terminal device using the received random-number identification information by the random-number identification means;

a confidential-information identification step of identifying the confidential information of the device terminal using the received confidential-information identification information by the confidential-information identification means;

a conversion step of generating a conversion value by converting a set of the identified confidential information and the random number using the same one-way function as that used by the terminal device by the conversion means; and

a device authentication step of granting device authentication to the terminal device using the received conversion value and the generated conversion value by the device authentication means.

9. An authentication method used by the service server according to claim 4, the service server including a computer having random-number acquisition means, random-number transmission means, reception means, random-number

identification means, authentication-information transmission means, and authentication-result reception means, the authentication method comprising:

a random-number acquisition step of acquiring a random number by the random-number acquisition means;

a random-number transmission step of transmitting the acquired random number to the terminal device by the random-number transmission means;

a reception step of receiving from the terminal device a conversion value generated using the confidential information and confidential-information identification information by the reception means;

a random-number identification step of identifying the random number transmitted to the terminal device by the random-number identification means;

an authentication-information transmission step of transmitting, to the authentication server, authentication information including the received conversion value, the confidential-information identification information, and the identified random number by the authentication-information transmission means; and

an authentication-result reception step of receiving from the authentication server a result of authentication based on the transmitted authentication information by the authentication-result reception means.

10. A terminal device method used by the terminal device receiving a service from the service server according to claim 4, the terminal device including a computer having random-number reception means, conversion means, and transmission means, the terminal device method comprising:

a random-number reception step of receiving a random number from the service server by the random-number reception means;

a conversion step of generating a conversion value by converting a set of the received random number and the confidential information by the use of a one-way function by the conversion means; and

a transmission step of transmitting the generated conversion value and confidential-information identification information for identifying the confidential information in the authentication server by the transmission means.

11. An authentication method used by the authentication server for granting device authentication to the device terminal when the service server according to claim 4 provides a service, the authentication server including a computer having reception means, confidential-information identification means, conversion means, and device authentication means, the authentication method comprising:

a reception step of receiving, from the service server, authentication information including a conversion value, confidential-information identification information, and a random number by the reception means;

a confidential-information identification step of identifying the confidential information of the terminal device by the use of the received confidential-information identification information by the confidential-information identification means;

a conversion step of generating a conversion value by converting a set of the received random number and the identified confidential information by the use of the same one-way function as that used by the terminal device by the conversion means; and

a device authentication step of granting device authenticating to the terminal device by the use of the received conversion value and the generated conversion value by the device authentication means.

12. A terminal device program in the terminal device that is granted device authentication in the device authentication system according to claim 1, the terminal device including a computer, the terminal device program realizing:

a reception function for receiving from the authentication server a random number and random-number identification information for identifying the random number;

a conversion function for generating a conversion value by converting a set of the received random number and the confidential information using a one-way function; and

a transmission function for transmitting the generated conversion value, the received random-number identification information, and confidential-information identification information for identifying the confidential information in the authentication server.

13. An authentication program in the authentication server for granting device authentication to the terminal device according to claim 2, the authentication server including a computer, the authentication program realizing:

a random-number acquisition function for acquiring a random number;

a transmission function for transmitting to the terminal device the acquired random number and random-number identification information for identifying the random number;

a reception function for receiving from the terminal device a conversion value, the random-number identification information, and confidential-information identification information;

a random-number identification function for identifying the random number transmitted to the terminal device using the received random-number identification information;

a confidential-information identification function for identifying the confidential information of the device terminal using the received confidential-information identification information;

a conversion function for generating a conversion value by converting a set of the identified confidential information and the random number using the same one-way function as that used by the terminal device; and

a device authentication function for granting device authentication to the terminal device using the received conversion value and the generated conversion value.

14. A service server program in the service server according to claim 4, the service server including a computer, the service server program realizing:

a random-number acquisition function for acquiring a random number;

a random-number transmission function for transmitting the acquired random number to the terminal device;

a reception function for receiving from the terminal device a conversion value generated using the confidential information and confidential-information identification information;

a random-number identification function for identifying the random number transmitted to the terminal device;

an authentication-information transmission function for transmitting, to the authentication server, authentication information including the received conversion value, the confidential-information identification information, and the identified random number; and

an authentication-result reception function for receiving from the authentication server a result of authentication based on the transmitted authentication information.

15. A terminal device program in the terminal device receiving a service from the service server according to claim 4, the terminal device including a computer, the terminal device program realizing:

a random-number reception function for receiving a random number from the service server;

a conversion function for generating a conversion value by converting a set of the received random number and the confidential information by the use of a one-way function; and

a transmission function for transmitting the generated conversion value and confidential-information identification information for identifying the confidential information in the authentication server.

16. An authentication program in the authentication server for granting device authentication to the device terminal when the service server according to claim 4 provides a

service, the authentication server including a computer, the authentication program realizing:

a reception function for receiving, from the service server, authentication information including a conversion value, confidential-information identification information, and a random number;

a confidential-information identification function for identifying the confidential information of the terminal device by the use of the received confidential-information identification information;

a conversion function for generating a conversion value by converting a set of the received random number and the identified confidential information by the use of the same one-way function as that used by the terminal device; and

a device authentication function for granting device authenticating to the terminal device by the use of the received conversion value and the generated conversion value.

17. A computer-readable recording medium including the device terminal program according to claim 12 or claim 15.

18. A computer-readable recording medium including the authentication program according to claim 13 or claim 16.

19. A computer-readable recording medium including the service server program according to claim 14.